Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 307 (2007) 373–385
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Minimal normal subgroups of transitive permutation groups of square-free degree

Edward Dobson[a], Aleksander Malnič[b,1], Dragan Marušič[b,c,*,1], Lewis A. Nowitz[d]

[a] Mississipi State University, PO Drawer MA Mississippi State, MS 39762, USA
[b] IMFM, University of Ljubljana, Jadranska 19, 1000 Ljubljana, Slovenia
[c] University of Primorska, Cankarjeva 6, 6000 Koper, Slovenia
[d] 2345 Broadway no. 526, New York, NY 100024-3213, USA

Received 19 May 2004; received in revised form 8 February 2005; accepted 26 September 2005
Available online 30 August 2006

Abstract

It is shown that a minimal normal subgroup of a transitive permutation group of square-free degree in its induced action is simple and quasiprimitive, with three exceptions related to A_5, A_7, and $\mathrm{PSL}(2, 29)$. Moreover, it is shown that a minimal normal subgroup of a 2-closed permutation group of square-free degree in its induced action is simple. As an almost immediate consequence, it follows that a 2-closed transitive permutation group of square-free degree contains a semiregular element of prime order, thus giving a partial affirmative answer to the conjecture that all 2-closed transitive permutation groups contain such an element (see [D. Marušič, On vertex symmetric digraphs, Discrete Math. 36 (1981) 69–81; P.J. Cameron (Ed.), Problems from the fifteenth British combinatorial conference, Discrete Math. 167/168 (1997) 605–615]).

Keywords: Transitive permutation group; 2-Closed group; Square-free degree; Semiregular automorphism; Vertex-transitive graph

1. Introductory remarks

There has recently been an increasing interest in the study of permutation groups of square-free degree and their respective (di)graphs. Apart from the fact that understanding the structure of such objects is interesting in its own right, an additional motivation stems from a problem posed by the third author [16], who asked for which natural numbers n there exists a non-Cayley vertex-transitive graph on n vertices. In [21,22], Praeger and McKay reduced this problem to square-free numbers. Moreover, drawing together work by several other people [8,12,13,17,18,20,23,24], the problem has now been settled except for those square-free numbers which are products of at least four primes. Affirmative results on whether an integer is a Cayley number usually rely upon some sort of structure theorem concerning an appropriate transitive subgroup of the full automorphism group of a graph. In such results, information about the orbits of a minimal normal subgroup (and of its recursive canonical quotient groups) is prominent, as are arithmetic conditions. See for example [6,12,15].

* Corresponding author. University of Primorska, Cankarjeva 6, 6000 Koper, Slovenia.
E-mail address: dragan.marusic@guest.arnes.si (D. Marušič).
1 Supported in part by "Agencija za raziskovalno dejavnost Republike Slovenije", research program P1-0285.

0012-365X/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2005.09.029

Recall that any transitive permutation group G is either primitive or imprimitive. Let us assume that G is of square-free degree n. If G is primitive, then Li and Seress [14] have recently produced a list containing all such groups. If G is imprimitive, then either G is quasiprimitive (all normal subgroups are transitive), or G contains an intransitive normal subgroup whose orbits form a complete block system of G. If G is quasiprimitive, then G has a faithful representation as a primitive group of degree dividing n, and so is also contained in the Li–Seress list.

The purpose of this paper is to begin to address the question of what can occur in the remaining case, namely, when G admits a complete block system formed by the orbits of an intransitive normal subgroup. As every nonsimple group contains a nontrivial normal subgroup, and so a minimal normal subgroup, we will investigate what a minimal normal subgroup of a transitive group of square-free degree must be. For completeness, our main results will hold for all transitive permutation groups of degree n, primitive or imprimitive, as it is an easy consequence of the O'Nan-Scott Theorem that a minimal normal subgroup of a primitive group is simple (see Lemma 2.1) for such n.

In this paper we show that a minimal normal subgroup of a transitive group of square-free degree, restricted to one of its orbits, is a simple group—with three exceptions. These are: an action of A_5^2 of degree 30, an action of A_7^2 of degree 105, and an action of $\mathrm{PSL}(2,29)^2$ of degree 6090 (Theorem 2.10). We then show if G is 2-closed, then the same result holds with no exceptions (Theorem 3.6). As an easy application of this last result we prove that every 2-closed group of square-free degree has a semiregular element (Theorem 4.1), thus giving a partial affirmative answer to the conjecture that all 2-closed transitive permutation groups contain such an element [1,15,19].

2. Minimal normal subgroups of square-free degree groups

Let G be a (finite) permutation group acting on a (finite) set Ω. If $H \leqslant G$ is a subgroup and $\Delta \subseteq \Omega$ a subset invariant under the action of H, we let H^{Δ} denote the restriction of H to Δ, and for $h \in H$ we let h^{Δ} denote the corresponding restriction of h to Δ. Let the above action of G be transitive and imprimitive and let $\mathscr{B}$ be a corresponding complete block system of G. Let $B \in \mathscr{B}$. By $\mathrm{Stab}_G(B) = \{g \in G \mid g(B) = B\}$ we denote the set-wise stabilizer of B in G, and by $G_{(B)}$ the point-wise stabilizer of B in G. By $\mathrm{fix}_G(\mathscr{B}) = \{g \in G \mid \text{for all } B \in \mathscr{B} : g(B) = B\}$ we denote the *fixer* of $\mathscr{B}$ in G, that is, the kernel of the action of G on $\mathscr{B}$. By $G/\mathscr{B}$ we denote the induced action of G on the set of blocks $\mathscr{B}$.

Lemma 2.1. *Let G be a quasiprimitive permutation group of composite square-free degree. Then* $\mathrm{soc}(G)$ *is a nonabelian simple group*.

Proof. Clearly, G is either primitive or G admits some nontrivial maximal complete block system $\mathscr{B}$ such that the action $G/\mathscr{B}$ of G on $\mathscr{B}$ is a faithful representation of G with no nontrivial blocks. In either case, G is isomorphic to a primitive group of square-free degree, say n (a divisor of the degree of the original action of G). Therefore the O'Nan-Scott Theorem (see [4, Theorem 4.1A]) implies the existence of a nonabelian simple group T such that either $\mathrm{soc}(G) = T$, or $\mathrm{soc}(G) = T^m$, $m \geqslant 2$ and G is of "diagonal type" with $n = |T|^{m-1}$. In the first case we are done. In the second case, as n is square-free, we must have $m = 2$. Consequently, the nonabelian simple group T is of square-free order. However,by [11, Corollary 9.4.1] any group of square-free order is metacyclic and thus solvable, a contradiction. □

Lemma 2.2. *Let G be a transitive permutation group of square-free degree with a complete block system $\mathscr{B}$, with blocks formed by the orbits of an intransitive normal subgroup of G. Let $B \in \mathscr{B}$. If* $\mathrm{Stab}_G(B)^B$ *is quasiprimitive, then* $\mathrm{fix}_G(\mathscr{B})^B$ *is quasiprimitive, too*.

Proof. If $|B|$ is prime, then $\mathrm{fix}_G(\mathscr{B})^B$ is of prime degree, and thus primitive and hence quasiprimitive. So we may assume that $|B|$ is composite. Since $\mathrm{fix}_G(\mathscr{B})$ is a (nontrivial) normal subgroup of $\mathrm{Stab}_G(B)$, it follows that $\mathrm{fix}_G(\mathscr{B})^B$ is a (nontrivial) normal subgroup of $\mathrm{Stab}_G(B)^B$. As $\mathrm{Stab}_G(B)^B$ is quasiprimitive, Lemma 2.1 implies that $\mathrm{soc}(\mathrm{Stab}_G(B)^B)$ is a nonabelian simple group, and hence the minimal normal subgroup of $\mathrm{Stab}_G(B)^B$. This together with the fact that $\mathrm{fix}_G(\mathscr{B})^B \lhd \mathrm{Stab}_G(B)^B$ implies that $\mathrm{soc}(\mathrm{fix}_G(\mathscr{B})^B) = \mathrm{soc}(\mathrm{Stab}_G(B)^B)$. Whence any normal subgroup of $\mathrm{fix}_G(\mathscr{B})^B$ must be transitive, as required. □

Lemma 2.3. *Let $1 \leqslant r < s < n$. Then $\binom{n}{r}$ and $\binom{n}{s}$ are not relatively prime.*

Table 1
Sporadic socles of primitive groups of square-free degree

soc(G)	Degree	Common factor
M_{11}	11, 55, 165	11
M_{12}	22, 77, 231, 330	11
M_{23}	253, 506, 1771	23
J_1	266, 1045, 1463, 2926	19

Table 2
Alternating socles of primitive groups of square-free degree

soc(G)	Degree	Comment
A_n	$\binom{n}{k}$, $1 \leqslant k \leqslant n-1$	Pair-wise common factor by Lemma 2.3
A_5	5, 6, 10	$6 \cdot 5$ is square-free
A_6	6, 10, 15, 20	Pair-wise common factors
A_7	7, 15, 21, 35	$7 \cdot 15$ is square-free
A_8	15, 35, 70, 105	5 common factor
A_{12}	66, 452	66 common factor
A_{18}	24310	Unique
A_{20}	190, 4199, 125970, 92378	19 common factor
A_{24}	1352078	Unique
A_{36}	2212562701384183 89602	Unique

Proof. Consider the equality

$$\binom{n}{s}\binom{s}{r} = \binom{n}{r}\binom{n-r}{s-r}.$$

If $\binom{n}{s}$ and $\binom{n}{r}$ are relatively prime, then $\binom{s}{r}$ is divisible by $\binom{n}{r}$, which contradicts the fact that $\binom{n}{r} > \binom{s}{r}$. Indeed, as $n-i+1 > s-i+1$ for all $1 \leqslant i \leqslant r$, we have $n!/(n-r)! > s!/(s-r)!$, or $\binom{n}{r} > \binom{s}{r}$. $\square$

Lemma 2.4. *If there are at least two primitive groups G_1 and G_2 of relatively prime square-free degrees such that* $\mathrm{soc}(G_1) = \mathrm{soc}(G_2)$, *then either*

(i) $\mathrm{soc}(G_1) = \mathrm{soc}(G_2) = A_5$ *and G_1 is of degree* 5 *and G_2 is of degree* 6; *or*
(ii) $\mathrm{soc}(G_1) = \mathrm{soc}(G_2) = A_7$ *and G_1 is of degree* 7 *and G_2 is of degree* 15; *or*
(iii) $\mathrm{soc}(G_1) = \mathrm{soc}(G_2) = \mathrm{PSL}(2, 29)$ *and G_1 is of degree* 203 *and G_2 is of degree* 30.

Proof. Our proof is based upon a recent result of Li and Seress [14] who give a list of all possibilities for primitive groups of square-free degree. (Note that Li and Seress do not claim that all of the groups on their list have the required properties, but that if the group has the required property, it is on the list. For example, according to Atlas [3], the group A_5 does not admit a primitive action of degree 20, and A_8 does not admit primitive actions of degrees 70 and 105.)

The list is broken into four parts, depending upon what family the socle of a primitive group falls into. For groups with exceptional socles, each such socle is the socle of a unique primitive group. For primitive groups with sporadic socle, Table 1 lists all such socles along with their degrees, and gives a common factor in each case. For primitive groups with alternating socles, Table 2 gives all such socles along with their degrees, as well as justification for A_5 and A_7 having two primitive representations of the required degrees. We are then left with considering primitive groups with classical socles. Table 3 lists those socles and degrees for which there is neither a unique primitive group of degree given by [14], nor those which a cursory inspection can eliminate. Where a straightforward computation will provide a common factor, these are listed in the comments in Table 3. We are then left with only consider $\mathrm{PSL}(2, q)$. All of these remaining cases can be handled easily, but there are a large number of cases to consider. We thus give these arguments separately below.

Table 3
Some classical socles of primitive groups of square-free degree

soc(G)	Degree	Comment
PSL(m, q)	$\dfrac{\Pi_{i=0}^{k-1}(q^{m-i}-1)}{\Pi_{i=1}^{k}(q^{i}-1)}$	$1 \leqslant k < m$
	$\dfrac{\Pi_{i=0}^{2k-1}(q^{m-i}-1)}{(\Pi_{i=1}^{k}(q^{i}-1))^2}$	$1 \leqslant k < m/2$
		$\dfrac{\Pi_{i=0}^{k-1}(q^{m-i}-1)}{\Pi_{i=1}^{k}(q^{i}-1)}$ a common factor
PSL$(2, q)$	$q(q+1)/2, q(q-1)/2$	q a common factor if q is odd $\dfrac{q}{2}$ a common factor if q is even
PSL$(2, q)$	$q_0(q_0^2+1)/2$	$q = q_0^2$ is odd
PSL$(2, q)$	$q(q^2-1)/24$	$q \equiv \pm 3 \pmod 8$
PSL$(2, q)$	$q(q^2-1)/48$	$q \equiv \pm 1 \pmod 8$
PSL$(2, q)$	$q(q^2-1)/120$	$q \equiv \pm 1 \pmod{10}$
PSp$(2m, q)$	$\dfrac{q^{2m}-1}{q-1}, \dfrac{(q^{2m}-1)(q^{2m-2}-1)}{(q^2-1)(q-1)}$	$\sum_{i=0}^{m-1} q^i$ a common factor
$\Omega(2m+1, q)$	$\dfrac{q^{2m}-1}{q-1}, \dfrac{(q^{2m}-1)(q^{2m-2}-1)}{(q^2-1)(q-1)}$	$\sum_{i=0}^{m-1} q^i$ a common factor
P$\Omega^-(2m, q)$	$\dfrac{(q^m+1)(q^{m-1}-1)}{q-1}, \dfrac{(q^m+1)(q^{2m-2}-1)(q^{m-2}-1)}{(q^2-1)(q-1)}$	q^m+1 a common factor
	$\dfrac{(q^m+1)(q^{2m-2}-1)(q^{2m-4}-1)(q^{m-3}-1)}{(q^3-1)(q^2-1)(q-1)}$	
P$\Omega^+(2m, q)$	$\dfrac{(q^m-1)(q^{m-1}+1)}{q-1}, \dfrac{(q^m-1)(q^{2m-2}-1)(q^{m-2}+1)}{(q^2-1)(q-1)}$	$q^{m-1}+1$ a common factor
	$\dfrac{(q^m-1)(q^{2m-2}-1)(q^{2m-4}-1)(q^{m-3}+1)}{(q^3-1)(q^2-1)(q-1)}$	

• PSL$(2, q)$ IN ACTIONS ON $q+1$ AND $q(q-1)/2$ POINTS: If q is odd, note that $\gcd(q+1, (q-1)/2) = 1$ if and only if $q \equiv 3 \pmod 4$. But then $q+1 \equiv 0 \pmod 4$ so the action of PSL$(2, q)$ on $q+1$ points is not square-free. If q is even, then $q(q-1)/2 \equiv 0 \pmod 4$ unless $q = 4$. Then $q+1 = 5$ and $q(q-1)/2 = 30$, and of course, 5 and 30 are not relatively prime.
• PSL$(2, q)$ IN ACTIONS ON $q+1$ AND $q(q+1)/2$ POINTS: A common factor is $q+1$ if q is even and $(q+1)/2$ if q is odd.
• PSL$(2, q)$ IN ACTIONS ON $q+1$ AND $q(q^2-1)/24$ OR $q(q^2-1)/48$ POINTS: Then $q \equiv \pm 3 \pmod 8$ or $q \equiv \pm 1 \pmod 8$. Note that these cannot happen simultaneously. In either case, $q+1 \equiv 0 \pmod 4$ so that $q+1$ is not square-free.
• PSL$(2, q)$ IN ACTIONS ON $q+1$ AND $q_0(q_0^2+1)/2$ POINTS: In this case q_0 is odd, so that $q = q_0^2$ is odd. Then $(q+1)/2$ is a common factor.
• PSL$(2, q)$ IN ACTIONS ON $q+1$ AND $q(q^2-1)/120$ POINTS: A common factor is $(q+1)/\gcd(q+1, 120)$, provided $q+1$ does not divide 120. We may therefore assume that $q+1$ divides 120, which occurs for $q \in \{9, 11, 29, 59, 119\}$. For $q = 9, 119$, it follows that 2 is a common factor of $q+1$ and $q(q^2-1)/120$, whereas for $q = 11, 19, 59$ we have that $q+1 \equiv 0 \pmod 4$. This leaves us with $q = 29$, which does indeed lead to two relatively prime square-free degree actions of PSL$(2, 29)$, namely on $30 = 2 \cdot 3 \cdot 5$ and $203 = 7 \cdot 29$ points.
• PSL$(2, q)$ IN ACTIONS ON $q(q+1)/2$ OR $q(q-1)/2$ AND $q_0(q_0^2+1)/2$, POINTS: Then q_0 must be odd, $q = q_0^2$, so that neither $q(q+1)/2$ nor $q(q-1)/2$ is square-free.
• PSL$(2, q)$ IN ACTIONS ON $q(q+1)/2$ OR $q(q-1)/2$ AND $q(q^2-1)/24$ OR $q(q^2-1)/48$ POINTS: First, as $q \equiv \pm 3 \pmod 8$ or $q \equiv \pm 1 \pmod 8$, we have that q is odd. Note that $q \neq 3$ as then $q(q^2-1)/24 = 1/4$ or $q(q^2-1)/48 = 1/2$.

Table 4
Primitive actions of A_5, A_7 and PSL(2, 29), extracted from ATLAS

G	Index of maximal subgroup	Maximal subgroup
A_5	5	A_4
	6	D_{10}
	10	S_3
A_7	7	A_6
	15	PSL(2, 7)
	21	S_5
	35	$(A_4 \cdot 3) : 2$
PSL(2, 29)	30	29 : 14
	203	A_5
	406	D_{30}
	435	D_{28}

If $q \equiv 0 \pmod 3$, then q is not square-free so that neither $q(q+1)/2$ nor $q(q-1)/2$ is square-free. On the other hand, if $q \not\equiv 0 \pmod 3$, then q is a common factor of $q(q+1)/2$ or $q(q-1)/2$ and $q(q^2-1)/24$ or $q(q^2-1)/48$.

• PSL$(2, q)$ IN ACTIONS ON $q(q+1)/2$ OR $q(q-1)/2$ AND $q(q^2-1)/120$ POINTS: First, as $q \equiv \pm 1 \pmod{10}$, we have that q is odd. Note that $q \neq 3, 5$ as then $q(q^2-1)/120 < 1$. If $q \equiv 0 \pmod 3$ or $q \equiv 0 \pmod 5$, then q is not square-free so that neither $q(q+1)/2$ nor $q(q-1)/2$ is square-free. On the other hand, if $q \not\equiv 0 \pmod 3$ and $q \not\equiv 0 \pmod 5$, then q is a common factor of $q(q+1)/2$ or $q(q-1)/2$ and $q(q^2-1)/120$.

• PSL$(2, q)$ IN ACTIONS ON $q_0(q_0^2+1)/2$ AND $q(q^2-1)/24$, $q(q^2-1)/48$, OR $q(q^2-1)/120$ POINTS: In this case q_0 is odd, and $q = q_0^2 \neq 3$ or 5. If 9 or 25 divide q, then q_0 is a common factor of $q(q^2-1)/24$, $q(q^2-1)/48$, or $q(q^2-1)/120$. If q is relatively prime to 9 and 25, then q divides $q(q^2-1)/24$, $q(q^2-1)/48$, and $q(q^2-1)/120$, so that none of these values are square-free.

• PSL$(2, q)$ IN ANY TWO ACTIONS ON $q(q^2-1)/24$, $q(q^2-1)/48$, OR $q(q^2-1)/120$ POINTS: The first two actions, as noted above, cannot occur simultaneously. If the first and last actions occur, then $q(q^2-1)/24$ is a common factor. If the second and last occur, then $\gcd(48, 120) = 24$ divides $q(q^2-1)$. Again, $q(q^2-1)/24$ is a common factor. □

The following well known fact is used below in the analysis of some particular actions of the groups A_5, A_7, and PSL(2, 29).

Lemma 2.5. *Let G be a transitive permutation group with a complete block system $\mathcal{B}$. Then the size of a block $B \in \mathcal{B}$ is equal to the index of some subgroup in the corresponding block stabilizer* $\mathrm{Stab}_G(B)$, *and hence divisible by the index of some maximal subgroup in* $\mathrm{Stab}_G(B)$.

Lemma 2.6. *Let the group A_5 admit two imprimitive actions of square-free degrees rd and $r'd'$ with respective blocks of sizes r and r' such that the induced actions of degrees d and d' are primitive. If* $\gcd(d, d') = 1$, *then $d = 5$ and $r \in \{3, 6\}$, and $d' = 6$ and $r' = 5$.*

Proof. The possible degrees of primitive actions are, by Table 4, equal to 5, 6 or 10. Since $\gcd(d, d') = 1$ it follows that $d = 5$ and $d' = 6$. The proof now follows combining Lemma 2.5 with the fact that the degrees rd and $r'd'$ are square-free, and the fact that the block stabilizer is A_4 for $d = 5$ and D_{10} for $d' = 6$. □

Lemma 2.7. *Let the group A_7 admit two imprimitive actions of square-free degrees rd and $r'd'$ with respective blocks of sizes r and r' such that the induced actions of degrees d and d' are primitive. If* $\gcd(d, d') = 1$, *then $d = 7$ and $r \leqslant 360$ is divisible by* 6, 10 *or* 15, *and $d' = 15$ and $r' \leqslant 168$ is divisible by* 7.

Proof. The possible degrees of primitive actions are, by Table 4, equal to 7, 15, 21 or 35. Since $\gcd(d, d') = 1$ it follows that $d = 7$ and $d' = 15$. The proof now follows combining Lemma 2.5 with the fact that the degrees rd and $r'd'$ are square-free, and the fact that the block stabilizer is A_6 for $d = 7$ and PSL(2, 7) for $d' = 15$. □

Lemma 2.8. *Let the group* $\mathrm{PSL}(2, 29)$ *admit two imprimitive actions of square-free degrees* rd *and* $r'd'$ *with respective blocks of sizes* r *and* r' *such that the induced actions of degrees* d *and* d' *are primitive. If* $\gcd(d, d') = 1$, *then* $d = 30$ *and* $r \leqslant 406$ *is divisible by* 2, 7 *or* 29, *and* $d' = 203$ *and* $r' \leqslant 60$ *is divisible by* 5, 6 *or* 10.

Proof. The possible degrees of primitive actions are, by Table 4, equal to 30, 203, 406 or 435. Since $\gcd(d, d') = 1$ it follows that $d = 30$ and $d' = 203$. The proof now follows combining Lemma 2.5 with the fact that the degrees rd and $r'd'$ are square-free, and the fact that the block stabilizer is $\mathbb{Z}_{29} \rtimes \mathbb{Z}_{14}$ for $d = 30$ and A_5 for $d' = 203$. □

Lemma 2.9. *Let* G *be a transitive group and* N *a normal subgroup of* G *such that the orbits of* N *form a complete block system* $\mathscr{B}$ *with blocks of square-free cardinality, and let* $N^B = \prod_{i=1}^{r} T_i$, *where the factors* T_i, $1 \leqslant i \leqslant r$, *are isomorphic simple groups. If* $r \geqslant 2$, *then no* T_i *is transitive*.

Proof. Observe first that since $r \geqslant 2$, the cardinality $|B|$ is necessarily composite, and hence each T_j is nonabelian. Suppose some T_i, $1 \leqslant i \leqslant r$, is transitive on B. Note that as $\mathscr{B}$ is formed by the orbits of N, it follows that $N^B = \prod_{i=1}^{r} T_i \leqslant \mathrm{fix}_G(\mathscr{B})^B$. Thus, $T_j \leqslant \mathrm{fix}_G(\mathscr{B})^B$ for every $1 \leqslant j \leqslant r$. As T_i is transitive and each T_j is normal in N^B, we have that for each $b' \in B$ there exists $h_{b'} \in T_i$ such that $h_{b'}^{-1}\mathrm{Stab}_{T_j}(b)h_{b'} = \mathrm{Stab}_{T_j}(b')$. However, as every element of T_i commutes with every element of T_j, it follows that $\mathrm{Stab}_{T_j}(b) = \mathrm{Stab}_{T_j}(b')$ for every $b' \in B$. The faithfulness of N^B then implies that $\mathrm{Stab}_{T_j}(b) = 1$, and hence T_j is semiregular for each $j \neq i$. As T_i is transitive, it follows that $|B|$ divides $|T_i|$ and hence $|B|$ divides $|T_j|$ for all j. Consequently, T_j is transitive and so regular for all $j \neq i$. This then implies that T_i is also regular. However, as $|B|$ is square-free, by [11, Corollary 9.4.1], T_i is metacyclic and hence solvable. □

If $\mathscr{D}$ and $\mathscr{C}$ are complete block systems of the group G such that for every $D \in \mathscr{D}$ there exists $C \in \mathscr{C}$ such that $D \subseteq C$, then we will write $\mathscr{D} \preccurlyeq \mathscr{C}$.

Theorem 2.10. *Let* G *be a transitive permutation group of square-free degree* n, *with a complete block system* $\mathscr{B}$ *having blocks of size* m *formed by the orbits of a* (*proper*, *intransitive*) *minimal normal subgroup* N *of* G. *Then for all blocks* $B \in \mathscr{B}$ (*simultaneously*) *precisely one of the following occurs*.

(i) N^B *is simple and thus quasiprimitive*; *or*
(ii) $m = 30$ *and* $N^B \cong A_5^2$, *with one copy of* A_5 *acting with* 6 *blocks of size* 5 *and the other copy of* A_5 *acting with* 5 *blocks of size* 6; *or*
(iii) $m = 105$ *and* $N^B \cong A_7^2$, *with one copy of* A_7 *acting with* 15 *blocks of size* 7 *and the other copy of* A_7 *acting with* 7 *blocks of size* 15; *or*
(iv) $m = 6090$ *and* $N^B \cong \mathrm{PSL}(2, 29)^2$, *with one copy of* $\mathrm{PSL}(2, 29)$ *acting with* 30 *blocks of size* 203 *and the other copy of* $\mathrm{PSL}(2, 29)$ *acting with* 203 *blocks of size* 30.

Proof. As N is a minimal normal subgroup of G, it follows by [10, Theorem 2.1.5] that N is either elementary abelian or a direct product of isomorphic nonabelian simple groups. If N is elementary abelian, then as n is square-free, m is prime. Whence N^B is isomorphic to $\mathbb{Z}_m$ and thus simple and quasiprimitive.

We may therefore assume that N and hence N^B is a direct product of isomorphic nonabelian simple groups, say $N^B = \prod_{i=1}^{r} T_i$, where $T_i \cong T_j$, $1 \leqslant i, j \leqslant r$, and m is composite. If $r = 1$, then clearly $N^B = T_1$ is simple and quasiprimitive.

Suppose now that $r \geqslant 2$. Consider two distinct factors T_{i_j} and T_{i_k} of N^B. By Lemma 2.9, neither T_{i_j} nor T_{i_k} is transitive on B. Then N^B admits complete block systems $\mathscr{C}_j$ and $\mathscr{C}_k$ formed by the orbits of T_{i_j} and T_{i_k}, respectively. Let $C_j \in \mathscr{C}_j$ and $C_k \in \mathscr{C}_k$ be such that $C_j \cap C_k$ is nonempty. Then $C_j \cap C_k$ is a block of N^B, and so together with its conjugate blocks forms a complete block system $\mathscr{D}$ of N^B. If $C_j \subseteq C_k$, then $\mathscr{C}_j \prec \mathscr{C}_k$ and both T_{i_j} and T_{i_k} are contained in $\mathrm{fix}_{N^B}(\mathscr{C}_k)^{C_k}$. But then $T_{i_k}^{C_k}$ is transitive on C_k, contradicting Lemma 2.9. Hence, $C_j \nsubseteq C_k$, and an analogous argument shows that $C_k \nsubseteq C_j$.

Let $|D| = a$, $D \in \mathscr{D}$, $|C_j| = ab$, and $|C_k| = ac$, $C_j \in \mathscr{C}_j$, $C_k \in \mathscr{C}_k$. Note that $C_j/\mathscr{D} \cap C_k/\mathscr{D}$ is a singleton. Hence, if $C \in \mathscr{C}_j/\mathscr{D}$ and $C' \in \mathscr{C}_k/\mathscr{D}$, then $C \cap C'$ is either empty or a singleton. Using the fact that T_{i_j} and T_{i_k} centralize each other it can be seen that m/a is divisible by bc. As m/a is square-free, it follows that $\gcd(b, c) = 1$. Then $T_{i_j}/\mathscr{D} \cong T_{i_j}$

is transitive on $C_j/\mathscr{D}$ and $T_{i_k}/\mathscr{D} \cong T_{i_k}$ is transitive on $C_k/\mathscr{D}$. Let $\mathscr{E}_j$ and $\mathscr{E}_k$ be complete block systems of $T_{i_j}/\mathscr{D}$ and $T_{i_k}/\mathscr{D}$ acting on $C_j/\mathscr{D}$ and $C_k/\mathscr{D}$, respectively, that consist of more than one block and whose block size is maximal. Then $(T_{i_j}/\mathscr{D})/\mathscr{E}_j \cong T_{i_j}$ is simple of square-free degree in its action on the blocks of $\mathscr{E}_j$ and $(T_{i_k}/\mathscr{D})/\mathscr{E}_k \cong T_{i_k}$ is simple of square-free degree in its action on the blocks of $\mathscr{E}_k$. Hence, $T \cong T_{i_j} \cong T_{i_k}$ is a nonabelian simple group with at least two actions of relatively prime square-free degree. By Lemma 2.4, there are exactly three pairs of such actions. (Note that, since $\gcd(b, c) = 1$, the sizes of $(C_j/\mathscr{D})/\mathscr{E}_j$ and $(C_k/\mathscr{D})/\mathscr{E}_k$ are also coprime numbers. This excludes, for instance, the possibility of degree 10 action when $T \cong A_5$.)

1. $T_{i_j} = T_{i_k} = A_5$, $(T_{i_j}/\mathscr{D})/\mathscr{E}_j$ is of degree 5 and $(T_{i_k}/\mathscr{D})/\mathscr{E}_k$ is of degree 6, or
2. $T_{i_j} = T_{i_k} = A_7$, $(T_{i_j}/\mathscr{D})/\mathscr{E}_j$ is of degree 15 and $(T_{i_k}/\mathscr{D})/\mathscr{E}_k$ is of degree 7, or
3. $T_{i_j} = T_{i_k} = \mathrm{PSL}(2, 29)$, $(T_{i_j}/\mathscr{D})/\mathscr{E}_j$ is of degree 30 and $(T_{i_k}/\mathscr{D})/\mathscr{E}_k$ is of degree 203.

If (1) occurs, then combining Lemma 2.6 with the facts that m is square-free and $\gcd(b, c) = 1$, we have that $\mathscr{D}$ as well as $\mathscr{E}_j$ and $\mathscr{E}_k$ must consist of singletons. Analogously, applying Lemma 2.7 if (2) occurs, or Lemma 2.8 if (3) occurs, we have in all cases that $\mathscr{D}$, $\mathscr{E}_j$ and $\mathscr{E}_k$ all consist of singletons.

It then only remains to show that $r = 2$. If (1) occurs then we may assume that, say, T_1 has degree 5 and T_2 has degree 6. If $r \geqslant 3$, then arguments above show that, on the one hand, T_3 must have degree 6 (if compared with T_1), and on the other hand, degree 5 (if compared with T_2), which is clearly impossible. Analogous arguments apply when (2) or (3) occur. Consequently, $r = 2$, completing the proof of Theorem 2.10. □

3. Minimal normal subgroups of 2-closures of square-free degree groups

The main aim of this section is to prove an analogue of Theorem 2.10 in the context of 2-closed groups. Following [25], the 2-*closure* $G^{(2)}$ of G is the largest subgroup of the symmetric group S_V having the same orbits on V^2 as G. Alternatively, $G^{(2)}$ is the intersection of the automorphism groups of all orbital digraphs associated with the action of G on V. The group G is said to be 2-*closed* if it coincides with $G^{(2)}$. We will show that possibilities (ii)–(iv) of Theorem 2.10 cannot occur for such groups. In the analysis of these possibilities, the concept of a pseudometric defined on a complete block system of a transitive permutation group arising from a normal subgroup will prove useful. We start with the following proposition.

Proposition 3.1. *Let $\mathscr{B}$ be a complete block system of a transitive group G arising from a normal subgroup N of G such that, for each pair of blocks $B, B' \in \mathscr{B}$, we have $N^B \cong N^{B'}$. Then*

(i) *for any two blocks $B, B' \in \mathscr{B}$ we have $|N_{(B)}^{B'}| = |N_{(B')}^{B}|$;*
(ii) *for any three blocks $B, B', B'' \in \mathscr{B}$ we have $|N_{(B)}^{B'}| \cdot |N_{(B')}^{B''}| \geqslant |N_{(B)}^{B''}|$.*

Proof. To prove (i), observe that $N^B \cong N/N_{(B)}$ and hence $N_{(B)}^{B'} \cong N_{(B)}/(N_{(B)} \cap N_{(B')})$. Thus,

$$|N_{(B)}^{B'}| = \frac{|N|}{|N^B|} \cdot \frac{1}{|N_{(B)} \cap N_{(B')}|}.$$

Switching the roles of B and B' and taking into account the fact that $|N^B| = |N^{B'}|$, we get $|N_{(B)}^{B'}| = |N_{(B')}^{B}|$, as required.

Next, to prove (ii), note that $x^{-1}N_{(B)}x = N_{(B)}$ for each $x \in N_{(B')}$. Therefore we can define a surjective mapping from the set $N_{(B)}^{B'} \times N_{(B')}^{B''}$ to $N_{(B)}^{B''}$ by letting the element $(x^{B'}, y^{B''})$ be mapped to the element $(y^{-1}xy)^{B''}$ for any two $x \in N_{(B)}$ and $y \in N_{(B')}$. The result follows. □

Let G be a transitive permutation group with a complete block system $\mathscr{B}$ such that $\mathrm{fix}_G(\mathscr{B})$ contains a subgroup $K \cong U^s$, for some $k \geqslant 1$, such that, for all blocks $B \in \mathscr{B}$, the restriction $K^B \cong U^r$, $1 \leqslant r \leqslant s$, acts transitively on B. Then in view of Proposition 3.1 we can define a pseudometric on $\mathscr{B}$ by letting

$$\mathrm{Dist}_K(B, B') = \log_{|U|} |K_{(B)}^{B'}|.$$

Table 5
The pseudometric refined

$N_{(B)}^{B'}$	1, see (*)	1, see (**)	$U \times 1$	$1 \times U$	$U \times 1$	$1 \times U$	$U \times U$
$N_{(B')}^{B}$	1, see (*)	1, see (**)	$U \times 1$	$1 \times U$	$1 \times U$	$U \times 1$	$U \times U$
Dist	0	0	1	1	1	1	2
Rdist	0^+	0^-	1^+	1^-	$1^\pm$	$1^\pm$	2

Clearly, by part (i) of Proposition 3.1, it follows that Dist_K is symmetric, whereas the triangle inequality follows from part (ii) of Proposition 3.1. We remark that the index K above is usually omitted if the group is clear from the context.

Coming back to the special situation dealt with in this section, we let G be a transitive permutation group of square-free degree n with a (nontrivial) complete block system $\mathscr{B}$ arising from the orbits of a minimal normal subgroup N. Moreover, we assume that one of parts (ii)–(iv) in Theorem 2.10 occurs. In other words, the restriction $N^B = U \times U$, $B \in \mathscr{B}$, is not quasiprimitive, where U is one of A_5, A_7 or PSL(2, 29), and the size m of blocks is 30, 105 or 6090, respectively. In any case, N^B contains a normal subgroup $U \times 1$ with orbits of size b and a normal subgroup $1 \times U$ with orbits of size c, where $b = 5$, 7 or 203, and $c = 6$, 15, or 30, respectively. (As we shall see in the proof of Theorem 3.6, these two block systems give rise to complete blocks systems of sizes b and c for the whole group G.)

In this special situation the above pseudometric Dist=Dist_N may be further "refined" as follows. First, as $N^B \cong U \times U$, the pseudometric Dist can attain only values 0, 1, and 2. Now for each pair of distinct blocks $B, B' \in \mathscr{B}$, the restrictions $N_{(B)}^{B'}$ and $N_{(B')}^{B}$ can be either 1, $U \times 1$, $1 \times U$ or $U \times U$. According to which of the cases we encounter between each pair, the pseudometric Dist is refined in the following way. We let the *refined distance* $\mathrm{Rdist}_N(B, B')$ (in short $\mathrm{Rdist}(B, B')$) *between B and B′ relative to N* attain one of the following values: 2, 1^+, 1^-, $1^\pm$, 0^+, or 0^-, as explained in detail below (see also Table 5) .

First, $\mathrm{Rdist}(B, B') = 2$ if $N_{(B)}^{B'}$ and hence $N_{(B')}^{B}$ is transitive. Second, $\mathrm{Rdist}(B, B') = 1^+$ if both $N_{(B)}^{B'}$ and $N_{(B')}^{B}$ have orbits of size b. Third, $\mathrm{Rdist}(B, B') = 1^-$ if both $N_{(B)}^{B'}$ and $N_{(B')}^{B}$ have orbits of size c. Fourth, $\mathrm{Rdist}(B, B') = 1^\pm$ if $N_{(B)}^{B'}$ has orbits of size b and $N_{(B')}^{B}$ has orbits of size c, or vice versa. Fifth (*), $\mathrm{Rdist}(B, B') = 0^+$ if $N_{(B)}^{B'} = 1$ and if H is a subgroup of N such that the restriction H^B has orbits of size $d \in \{b, c\}$ then the restriction $H^{B'}$ also has orbits of size d. Finally (**), we say that $\mathrm{Rdist}(B, B') = 0^-$ if $N_{(B)}^{B'} = 1$ and if H is a subgroup of N such that H^B has orbits of size b, then $H^{B'}$ has orbits of size c, or vice versa.

In the next lemma we analyze the structure of a digraph Γ arising from the action of a transitive group G with a (proper, intransitive) minimal normal subgroup N and the corresponding complete block system $\mathscr{B}$ satisfying the usual assumptions. Given disjoint subsets W and W' of $V(\Gamma)$ we let $\Gamma[W, W'] = [W, W']$ denote the digraph induced by all the (directed) edges in Γ between some vertex in W and some vertex in W'. A particular instance of this situation when W and W' coincide with two blocks B and B' in $\mathscr{B}$, will be of special interest to us. In particular, we denote the bipartite digraph that consists of every directed edge from a vertex of B to a vertex of B' by $\overrightarrow{K}_{bc,bc}$, and the bipartite digraph that consists of every directed edge from a vertex of B' to a vertex of B by $\overleftarrow{K}_{bc,bc}$. Next, by the digraph $K_{r,r}$, we mean the graph with two bipartition classes R, R' of size r, such that $\vec{xy}$, $\vec{yx}$ is a directed edge in $K_{r,r}$ for every $x \in R$ and $y \in R'$. Given digraphs X and Y we let $X \wr Y$ denote the wreath product of X by Y. Finally, the complement of a digraph X will be denoted by $\bar{X}$.

Lemma 3.2. *Let Γ be a digraph of square-free order n, let G be a subgroup of* $\mathrm{Aut}(\Gamma)$ *acting transitively on* $V(\Gamma)$, *and let $\mathscr{B}$ be the complete block system of G formed by the orbits of a (proper, intransitive) minimal normal subgroup N of G such that N^B, $B \in \mathscr{B}$ is not quasiprimitive. If there are distinct blocks $B, B' \in \mathscr{B}$ with* $\mathrm{Rdist}(B, B') \neq 0^+$ *such that there is a directed edge between some vertex of B and some vertex of B′, then the digraph* $[B, B']$ *is given in Table 6.*

Proof. Let $u \in B$ and $v \in B'$. We shall distinguish the following different cases.

Table 6
The subgraph $[B, B']$ if $\mathrm{Rdist}(B, B') \neq 0^+$

$\mathrm{Rdist}(B, B')$	$[B, B']$	Comment
0^-	$K_{bc,bc}$, $\vec{K}_{bc,bc}$, $\overleftarrow{K}_{bc,bc}$	
1^+	$X \wr \bar{K}_b$	$X \leqslant K_{c,c}$
1^-	$Y \wr \bar{K}_c$	$Y \leqslant K_{b,b}$
$1^{\pm}$	$K_{bc,bc}$, $\vec{K}_{bc,bc}$, $\overleftarrow{K}_{bc,bc}$	
2	$K_{bc,bc}$, $\vec{K}_{bc,bc}$, $\overleftarrow{K}_{bc,bc}$	

Case 1: $\mathrm{Rdist}(B, B') = 2$. If $\vec{uv} \in E([B, B'])$, then as $N^{B'}_{(B)}$ is transitive, $\vec{uy} \in E([B, B'])$ for every $y \in B'$. As N^B and $N^{B'}$ are transitive, $\vec{xy} \in E([B, B'])$ for every $x \in B$, $y \in B'$. An analogous argument will show that if $\vec{vu} \in E([B, B'])$, then $\vec{yx} \in E([B, B'])$ for every $x \in B$, $y \in B'$. Thus $[B, B'] = K_{bc,bc}$, $\vec{K}_{bc,bc}$, or $\overleftarrow{K}_{bc,bc}$.

Case 2: $\mathrm{Rdist}(B, B') = 1^{\pm}$. With no loss of generality suppose that $N^B_{(B')}$ has orbits of size b and $N^{B'}_{(B)}$ has orbits of size c. Let $\mathcal{O}$ be the orbit of $N^B_{(B')}$ of size b that contains u and $\mathcal{O}'$ the orbit of $N^{B'}_{(B)}$ of size c that contains v. If $\vec{uv} \in E[B, B']$, then applying the action of $N_{(B)}$, clearly $\vec{uy} \in E([B, B'])$ for every $y \in \mathcal{O}'$. Similarly, applying the action of $N_{(B')}$, it follows that $\vec{xv} \in E([B, B'])$ for every $x \in \mathcal{O}$. In other words, all of the edges initiating in $\mathcal{O}$ and terminating in $\mathcal{O}'$ are in the $[\mathcal{O}, \mathcal{O}']$. Analogously, the same holds for any pair of adjacent orbits of $N^B_{(B')}$ and $N^{B'}_{(B)}$ in B and B', respectively. We conclude that, on the one hand, $\deg^+_{[B,B']}(u) = k_1 c$ is a multiple of c, and on the other hand $\deg^-_{[B,B']}(v) = k_2 b$ is a multiple of b. As N^B and $N^{B'}$ are transitive, it follows that $\deg^+_{[B,B']}(x) = k_1 c$ for each $x \in B$ and $\deg^-_{[B,B']}(y) = k_2 b$ for each $y \in B'$. Counting the directed edges from B to B' in two ways and using the fact that $\gcd(b, c) = 1$, we conclude that $\vec{xy} \in E([B, B'])$ for every $x \in B$, $y \in B'$. The remaining possibilities (for the direction of the edges between two orbits of H) to complete this case are exactly analogous, and the result follows.

Case 3: $\mathrm{Rdist}(B, B') = 0^-$. Let, without loss of generality, $H \leqslant N$ be such that H^B has orbits of size b. By definition, $H^{B'}$ has orbits of size c. Then $H^B = U \times 1$ and $H^{B'} = 1 \times U$. Let $\mathcal{O}$ be the orbit of H^B on B of size b that contains u, and let $\mathcal{O}'$ the orbit of $H^{B'}$ on B' of size c that contains v. Then there exists an element $h \in H$ of prime order p, which is 5, 7 or 29, respectively, depending on whether U is A_5, A_7 or $\mathrm{PSL}(2, 29)$, such that $h^{\mathcal{O}}$ is semiregular whereas $h(v) = v$. (Note that the semiregularity of h^B when $b = 203$ follows from the fact that a transitive permutation group of degree kp, $k < p$, has a semiregular element, see [15].) If $\vec{uv} \in E([B, B'])$, then $\vec{xv} \in E([B, B'])$ for every x belonging to the same orbit of h as u. If U is either A_5 or A_7, then applying the action of H on $\mathcal{O}$ and $\mathcal{O}'$ it follows that all of the directed edges initiating in $\mathcal{O}$ and terminating in $\mathcal{O}'$ are in $[\mathcal{O}, \mathcal{O}']$. Suppose that $U = \mathrm{PSL}(2, 29)$. Then $\mathcal{O}$ consists of 7 orbits of $h^{\mathcal{O}}$ of length 29, and a directed edge initiating in a vertex in any of these orbits and terminating at $v$implies the existence of all directed edges from vertices in that orbit to v. Consequently, $\deg^-_{[\mathcal{O},\mathcal{O}']}(v) = 29 \cdot k$. Since $\mathcal{O}'$ is an orbit of H, we have that $\deg^-_{[\mathcal{O},\mathcal{O}']}(y) = 29 \cdot k$ for all $y \in \mathcal{O}'$. Let $\deg^+_{[\mathcal{O},\mathcal{O}']}(x) = l$, where $x \in \mathcal{O}$. Counting the number of directed edges from $\mathcal{O}$ to $\mathcal{O}'$ in two different ways we get that $7 \cdot 29 \cdot l = 30 \cdot 29 \cdot k$. Hence $l = 30$ and $k = 7$. In other words, all of the directed edges initiating in $\mathcal{O}$ and terminating in $\mathcal{O}'$ are in $[\mathcal{O}, \mathcal{O}']$ (as in the case when U is A_5 or A_7). Analogously (for U equal either to A_5, A_7 or $\mathrm{PSL}(2, 29)$), the same holds for any pair or adjacent orbits of H^B and $H^{B'}$ on B and B', respectively. From here on the argument is exactly the same as in Case 2. The remaining possibilities (for the direction of the edges between two orbits of H) to complete this case are exactly analogous, and the result follows.

Case 4: $\mathrm{Rdist}(B, B') \in \{1^+, 1^-\}$. As both of the subcases are analogous we only give the proof when $\mathrm{Rdist}(B, B') = 1^+$. Thus, both $N^B_{(B')}$ and $N^{B'}_{(B)}$ have orbits of size b. In particular, let $\mathcal{O}$ and $\mathcal{O}'$ be the orbits of $N^B_{(B')}$ and $N^{B'}_{(B)}$ that contain u and v, respectively. If $\vec{uv} \in E(\Gamma)$, then $\vec{uy} \in E(\Gamma)$ for every $y \in \mathcal{O}'$ and $\vec{xv} \in E(\Gamma)$ for every $x \in \mathcal{O}$. Arguing analogously for each of the edges $\vec{uy}$ and $\vec{xv}$, we have that $\vec{xy} \in E(\Gamma)$ for every $x \in \mathcal{O}$ and $y \in \mathcal{O}'$. We conclude that between any orbit of $N^B_{(B')}$ and any orbit of $N^{B'}_{(B)}$, we have either all directed edges or no directed edges. Whence $[B, B'] \leqslant X \wr \bar{K}_b$. (We remark that much information can be obtained about the possible form of X, but we will not need that information here. For example, if X is a graph, then $X = K_{c,c}$, $K_{c,c} - I$, or I, where I is a 1-factor.) The other possibilities (for the direction of the edges between $\mathcal{O}'$ and $\mathcal{O}$) are taken care of in an analogous way. $\square$

Let G be a transitive permutation group that admits a complete block system $\mathscr{B}$ of blocks of size m, formed by the orbits of some nontrivial and intransitive normal subgroup N of G. Furthermore, assume that the restriction $\mathrm{fix}_G(\mathscr{B})^B$ is quasiprimitive for every block $B \in \mathscr{B}$.

Define an equivalence relation $\equiv$ on the set of blocks $\mathscr{B}$ by letting $B \equiv B'$ if and only if $\mathrm{fix}_G(\mathscr{B})_{(B)}$ and $\mathrm{fix}_G(\mathscr{B})_{(B')}$, the respective kernels of the restrictions of $\mathrm{fix}_G(\mathscr{B})$ to B and to B', coincide. Denote the equivalence classes of the relation $\equiv$ by $C_0, \ldots, C_a$, and let $E_i = \bigcup_{B \in C_i} B$. The following result was proven in [5] in the case where m is a prime. It is straightforward to generalize this result to m being composite provided that $\mathrm{fix}_G(\mathscr{B})^B$ is quasiprimitive for every $B \in \mathscr{B}$ and the action of $\mathrm{fix}_G(\mathscr{B})$ is not faithful.

Lemma 3.3 (*Dobson [5]*). *Let $\vec{X}$ be a vertex-transitive digraph for which $G \leqslant \mathrm{Aut}(\vec{X})$ as above. Then $\mathrm{fix}_G(\mathscr{B})^{E_i} \leqslant \mathrm{Aut}(\vec{X})$ for every $0 \leqslant i \leqslant a$ (here if $g \in \mathrm{fix}_G(\mathscr{B})$, then it is meant that $g^{E_i}(x) = g(x)$ if $x \in E_i$ and $g^{E_i}(x) = x$ if $x \notin E_i$). Furthermore, $\{E_i : 0 \leqslant i \leqslant a\}$ is a complete block system of G.*

As the 2-closure $G^{(2)}$ of a group G is equal to the intersection of the automorphism groups of the orbital digraphs of G, we have the following.

Corollary 3.4. *Let G be a transitive group as in the paragraph preceding the statement of Lemma* 3.3. *Then $\mathrm{fix}_G(\mathscr{B})^{E_i} \leqslant G^{(2)}$ for every $0 \leqslant i \leqslant a$ (here if $g \in \mathrm{fix}_G(\mathscr{B})$, then it is meant that $g^{E_i}(x) = g(x)$ if $x \in E_i$ and $g^{E_i}(x) = x$ if $x \notin E_i$). Furthermore, $\{E_i : 0 \leqslant i \leqslant a\}$ is a complete block system of G.*

The following lemma will be needed in the proof of Theorem 3.6.

Lemma 3.5. *Let G be a transitive permutation group of square-free degree n, and let $\mathscr{B}_1$ and $\mathscr{B}_2$ be complete block systems arising from the orbits of normal subgroups N_1 and N_2 of G. If the blocks in $\mathscr{B}_1$ and $\mathscr{B}_2$ are of equal size, then $\mathscr{B}_1$ and $\mathscr{B}_2$ coincide.*

Proof. Let m be the common size of the blocks in $\mathscr{B}_1$ and $\mathscr{B}_2$. The result is clear if $m = 1$ or $m = n$ for then both block systems are trivial. We may therefore assume that $1 < m < n$. Suppose that $\mathscr{B}_1 \neq \mathscr{B}_2$. Then $N_1/\mathscr{B}_2 \neq 1$, forcing $N_1/\mathscr{B}_2$ to be a nontrivial normal subgroup of $G/\mathscr{B}_2$. The orbits of $N_1/\mathscr{B}_2$ are non-singleton, of size a divisor of m, and form a complete block system of $G/\mathscr{B}_2$. But $|G/\mathscr{B}_2| = n/m$, and is divisible by the size of the orbits of $N_1/\mathscr{B}_2$. However, as n is square-free, we have $\gcd(n/m, m) = 1$, a contradiction. $\square$

Theorem 3.6. *Let G be a transitive permutation group of square-free degree n, with a complete block system $\mathscr{B}$ formed by the orbits of a (proper, intransitive) minimal normal subgroup N of the* 2-*closure $G^{(2)}$. Then N^B is a simple group for every $B \in \mathscr{B}$.*

Proof. Let $m = |B|$, $B \in \mathscr{B}$. Let us assume, by way of contradiction, that N^B, $B \in \mathscr{B}$ is not simple. Then in view of Theorem 2.10 it follows that $m = 30$ and $N^B \cong A_5^2$, or $m = 105$ and $N^B \cong A_7^2$, or $m = 6090$ and $N^B \cong \mathrm{PSL}(2, 29)^2$.

First observe that N^B admits complete block systems $\mathscr{C}_B$ with blocks of size b and $\mathscr{D}_B$ with blocks of size c formed by the orbits of its normal subgroups $U \times 1$ and $1 \times U$, respectively. As conjugation of N^B by elements of $\mathrm{Stab}_G(B)^B$ induces an automorphism of N^B we have that $g^{-1}(U \times 1)g \lhd N^B$ for every $g \in \mathrm{Stab}_G(B)^B$. As the size of the orbits of $U \times 1$ are preserved by conjugation, we have that the orbits of $g^{-1}(U \times 1)g$ form a complete block system of N^B with blocks of size b. By Lemma 3.5, this complete block system is precisely $\mathscr{C}_B$. Hence, $g^{-1}(U \times 1)g \leqslant \mathrm{fix}_{N^B}(\mathscr{C}_B) = U \times 1$ so that $(U \times 1) \lhd \mathrm{Stab}_G(B)^B$. We conclude that $\mathrm{Stab}_G(B)^B$ admits $\mathscr{C}_B$ as a complete block system, so that by [4, Exercise 1.5.10] G admits a complete block system $\mathscr{C}$ of n/b blocks of size b. Exactly similar arguments will show that G also admits a complete block system $\mathscr{D}$ of n/c blocks of size c.

For convenience, we identify the set upon which G acts with $\mathbb{Z}_{n/m} \times \mathbb{Z}_b \times \mathbb{Z}_c$ so that $\mathscr{B} = \{\{(i, j, k) : j \in \mathbb{Z}_b, k \in \mathbb{Z}_c\} : i \in \mathbb{Z}_{n/m}\}$. Consider the group $K = \{(i, j, k) \to (i, \omega(j), k) : \omega \in U\}$. (Note that the restriction of K to each block $B \in \mathscr{B}$ is isomorphic to $U \times 1$.) It suffices to show that if Γ is an orbital digraph of G, then K is a subgroup of $\mathrm{Aut}(\Gamma)$. Namely, suppose that we have shown K is a subgroup of $\mathrm{Aut}(\Gamma)$. Let $M = \langle G, K \rangle$. As $K \leqslant M$, we then have that $\mathrm{fix}_M(\mathscr{C}) \neq 1$. If $K \leqslant \mathrm{Aut}(\Gamma)$ for every orbital digraph Γ of G, then $M \leqslant G^{(2)}$. As any complete block system of G is also a complete block system of $G^{(2)}$, we then have that $\mathrm{fix}_{G^{(2)}}(\mathscr{C}) \neq 1$. This, in turn, implies that $\mathrm{fix}_{G^{(2)}}(\mathscr{C})$ is a nontrivial normal subgroup of $G^{(2)}$, and so contains a minimal normal subgroup of $G^{(2)}$. As $\mathrm{fix}_K(\mathscr{C}) = U$, the result then follow by contradiction. So we now just show that K is indeed a subgroup of $\mathrm{Aut}(\Gamma)$.

Let Γ be an orbital digraph of G with $\vec{uv} \in E(\Gamma)$. If u and v belong to the same block $B \in \mathscr{B}$, then Γ is disconnected with $S_{n/bc} \wr (U \times U) \leqslant \mathrm{Aut}(\Gamma)$. It is then clear that $K \leqslant \mathrm{Aut}(\Gamma)$. We may therefore suppose that $u \in B$, $v \in B'$, and $B, B' \in \mathscr{B}$ are distinct blocks.

We shall distinguish various cases depending on which of the values the refined distance $\mathrm{Rdist}(B, B')$ takes.

Case 1: $\mathrm{Rdist}(B, B') \in \{0^-, 1^\pm, 2\}$. Let $u \in B$ and $v \in B'$. If $\mathrm{Rdist}(B, B') = 0^-$, $1^\pm$, or 2, then every orbital digraph of G that contains either $\vec{uv}$ or $\vec{vu}$ will by Lemma 3.2 be isomorphic to $X \wr \bar{K}_{bc}$, where X is a vertex-transitive digraph of order n/m. Then $\mathrm{Aut}(X) \wr S_{bc} \leqslant \mathrm{Aut}(\Gamma)$ and as it is easily seen that K is a subgroup of $\mathrm{Aut}(X) \wr S_{bc}$, we have that $K \leqslant \mathrm{Aut}(\Gamma)$.

Case 2: $\mathrm{Rdist}(B, B') = 1^+$. By Lemma 3.2, Γ is isomorphic to $X \wr \bar{K}_b$, where X is a vertex-transitive digraph of order n/b. Clearly then $K \leqslant \mathrm{Aut}(\Gamma)$.

Case 3: $\mathrm{Rdist}(B, B') = 1^-$. By Lemma 3.2, Γ is isomorphic to $X \wr \bar{K}_c$, where X is a vertex-transitive digraph of order n/c. Let $x \in N$. Then $x(i, j, k) = (i, \omega_i(j), \lambda_i(k))$, where each $\omega_i \in U$ (in its action on b points) and $\lambda_i \in U$ (in its action on c points). As $(1 \times U)^B \leqslant \mathrm{Aut}(\Gamma)$ for every $B \in \mathscr{B}$, we have that the function $\tilde{x}$ given by $\tilde{x}(i, j, k) = (i, j, \lambda_i(k))$ is contained in $\mathrm{Aut}(\Gamma)$. Thus the function $\hat{x}$ given by $\hat{x}(i, j, k) = (i, \omega_i(j), k)$ is also contained in $\mathrm{Aut}(\Gamma)$. Let $R = \langle \hat{x} : x \in N \rangle$. Define an equivalence relation $\equiv$ on $\mathscr{B}$ by $B_1 \equiv B_2$ if and only if the stabilizer in R of a point in B_1 is the stabilizer in R of a point in B_2, $B_1, B_2 \in \mathscr{B}$. It is easily seen that the equivalence classes of $\equiv$ form a complete block system $\mathscr{E}$ of M. Furthermore, by Corollary 3.4, we have that $R^E \subseteq M$ for every $E \in \mathscr{E}$. Note that R^E is a faithful representation of $(U \times 1)^{B_1}$. Let $S = \{R^E : E \in \mathscr{E}\}$. Note that S is indeed a group, and $S \leqslant \mathrm{Aut}(\Gamma)$. We now show that in this case, we must have $\mathrm{fix}_S(\mathscr{C})^C$ is equivalent to $\mathrm{fix}_S(\mathscr{C})^{C'}$ for every $C, C' \subseteq E \in \mathscr{E}$, and $C, C' \in \mathscr{C}$. Note that this will establish the result, as it will then follow that for every $B_1, B_2 \in \mathscr{B}$ such that $B_1, B_2 \subseteq E$, and $s \in S^E$, we have $s^{B_1} = s^{B_2}$ as $(U \times 1)^{B_1}$ is equivalent to $(U \times 1)^{B_2}$. This then implies that $K \leqslant S \leqslant \mathrm{Aut}(\Gamma)$.

According to the ATLAS [3], the actions of A_5 on 5 points and A_7 on 7 points are unique up to equivalence, while there are two inequivalent actions of PSL(2, 29) on 203 points. We thus need only consider the case when $b = 203$. We will proceed by contradiction, and assume that if $b = 203$, then there exists $B_1, B_2 \subseteq E$ such that $(U \times 1)^{B_1}$ is inequivalent to $(U \times 1)^{B_2}$.

For $E \in \mathscr{E}$, define a relation $\mathscr{R}_E$ on $\{C \in \mathscr{C} : C \subseteq E\}$ by $C \; \mathscr{R}_E \; C'$ if and only if $\mathrm{fix}_S(\mathscr{C})^C$ is equivalent to $\mathrm{fix}_S(\mathscr{C})^{C'}$. It is easy to see that $\mathscr{R}_E$ is an equivalence relation. By [4, Lemma 1.6B], we have that if $C \; \mathscr{R}_E \; C'$ then $T \leqslant \mathrm{fix}_S(\mathscr{C})$ is the stabilizer of a point in C if and only if T is the stabilizer of a point in C', where $C, C' \in \mathscr{C}$ such that $C, C' \subseteq E$. Let $g \in \mathrm{Stab}_G(E)$, and T the stabilizer of a point in $C \subseteq E$, and $C \in \mathscr{C}$. Let $C' \; \mathscr{R}_E \; C$. As conjugation maps the stabilizer of a point to the stabilizer of a point, we have that $g^{-1}Tg$ is the stabilizer of a point in $g(C)$, and $g^{-1}Gg$ is the stabilizer of a point in $g(C')$, so that $g(C) \; \mathscr{R}_E \; g(C')$. By [4, Exercise 1.5.4], we have that the equivalence classes of $\mathscr{R}_E$ are blocks of $\mathrm{Stab}_G(E)/\mathscr{C}$. It is easy to see that if $C, C' \in \mathscr{C}$ and $C, C' \subseteq B \in \mathscr{B}$, then $C \; \mathscr{R}_E \; C'$. Hence c divides the size of an equivalence class of $\mathscr{R}_E$. Furthermore, as PSL(2, 29) has exactly two inequivalent representations, we must also have that there are exactly two equivalence classes of $\mathscr{R}_E$. But if $U = \mathrm{PSL}(2, 29)$, $c = 30$, so that 4 divides n, a contradiction.

Case 4: $\mathrm{Rdist}(B, B') = 0^+$. First of all, the pseudometric Dist is preserved under the action of G. Therefore, $\mathrm{Dist}(g(B), g(B')) = 0$ for all $g \in G$. Furthermore, since the argument in Case 1 applies if $\mathrm{Rdist}(g(B), g(B')) = 0^-$ for some $g \in G$, we may assume that $\mathrm{Rdist}(g(B), g(B')) = 0^+$ for all $g \in G$. Consider the connected component of Γ containing the block B, and let H be the subgroup of N such that $H^B = U \times 1$. By definition of the refined distance 0^+ it follows that $H^{B''} = U \times 1$ for each block B'' belonging to the same connected component as B. Arguing as in Case 3, we have that H^B is equivalent to $H^{B''}$ for any block B'' that is contained in the same connected component of Γ as B. Doing the same for each connected component we infer that K is indeed a subgroup of $\mathrm{Aut}(\Gamma)$. $\square$

4. Semiregular elements

As an application of Theorem 2.10, we now prove that every 2-closed group of square-free degree has a nontrivial semiregular element. Recall that an element is *semiregular* if all of its orbits have equal size. A permutation group G is called *elusive* if it is transitive and has no nontrivial semiregular element. The name is intended to suggest that such groups appear to be quite rare. The first example of such a group was given in [7]. Let p be a Mersenne prime and let

G be the group consisting of all affine transformations of $GF(p^2)$ of the form $x \mapsto ax + b$, where $a, b \in GF(p^2)$ and $a \neq 0$, and let H be the subgroup consisting of these transformations for $a, b \in GF(p)$. Then the left action of G on the set of left cosets of H gives rise to a transitive permutation group of degree $p(p+1)$ whose every element of prime order fixes some point.

The problem of existence of nontrivial semiregular elements first arose in a graph-theoretic context. Namely, in 1981 [15, Problem 2.4] the third author asked whether the automorphism group of an arbitrary vertex-transitive digraph contains such an element. We remark that there are no known examples of 2-closed groups that are elusive, so the now commonly accepted version of this question involves the whole class of 2-closed transitive groups and is due to Klin [1]. Until very recently, only a few partial results were known. The interested reader is referred to [2] for an account of this problem.

The strategy of the proof of Theorem 4.1 involves a clear distinction between transitive permutation groups of square free degree which do have and those which do not have an intransitive nontrivial normal subgroup. In this context, a recent result of Giudici [9, Theorem 1.1] which implies that a quasiprimitive group of square-free degree is non-elusive, allows us a restriction to imprimitive permutation groups with an intransitive nontrivial normal subgroup. (While editing this paper, the authors were informed that M. Giudici has obtained another proof of this result.)

Theorem 4.1. *Every 2-closed group of square-free degree is non-elusive.*

Proof. In view of [9, Theorem 1.1] we may assume that if G is a 2-closed elusive group of square-free degree then G is not quasiprimitive. Hence, there exists $N \lhd G$ such that N is nontrivial and intransitive. We choose N to be minimal with respect to this property. Then the orbits of N form a complete block system $\mathscr{B}$. By Theorem 3.6, we have that N^B is a simple group for every $B \in \mathscr{B}$. Then N^B is quasiprimitive for each $B \in \mathscr{B}$. Hence, N^B contains semiregular element α_B of prime order p for every $B \in \mathscr{B}$. By Corollary 3.4, there exists a complete block system $\mathscr{E}$ of G (the unions of the equivalence classes of $\equiv$) such that $\mathrm{fix}_G(\mathscr{B})^E \leqslant G^{(2)}$ for all $E \in \mathscr{E}$. As the blocks of $\mathscr{E}$ are unions of the equivalence classes of $\equiv$, $(\mathrm{fix}_G(\mathscr{B})^E)^B$ is a faithful representation of $\mathrm{fix}_G(\mathscr{B})^E$ for every $B \in \mathscr{B}$ such that $B \subseteq E$. Hence $(N^E)^B$ is a faithful representation of N^E for every $B \in \mathscr{B}$ such that $B \subseteq E$. Furthermore, if $B, B' \in \mathscr{B}$, then N^B is permutation isomorphic to $N^{B'}$ as these two groups are conjugate. Hence, if $B, B' \in \mathscr{B}$ and $B, B' \subseteq E$, then $(N^E)^B$ is permutation isomorphic to $(N^E)^{B'}$. For each $E_i \in \mathscr{E}$, let $B_i \in \mathscr{B}$ such that $B_i \subseteq E_i$. Let $\alpha_i \in \mathrm{fix}_G(\mathscr{B})$ be $\alpha_i = \alpha_{B_i}^{E_i}$. Then α_i^E is semiregular of order p. Hence $\prod_{i=0}^{a} \alpha_i \in \mathrm{fix}_G(\mathscr{B})$ is semiregular of order p. $\square$

Albeit a small step towards a complete settlement of the above conjecture, Theorem 4.1 implies that the set of *non-elusive* numbers, that is, those numbers n, for which every 2-closed transitive permutation group of degree n is non-elusive, has positive density in the set of natural numbers as the set of square-free integers has density $6/\pi^2$ in the set of natural numbers.

Acknowledgment

The authors are indebted to the anonymous referee for suggestions that have improved the clarity of this paper.

References

[1] P.J. Cameron (Ed.), Problems from the fifteenth British combinatorial conference, Discrete Math. 167/168 (1997) 605–615.
[2] P.J. Cameron, M. Giudici, W.M. Kantor, G.A. Jones, M.H. Klin, D. Marušič, L.A. Nowitz, Transitive permutation groups without semiregular subgroups, J. London Math. Soc. 66 (2002) 325–333.
[3] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, Atlas of finite groups, Oxford University Press, Eynsham, 1985.
[4] J.D. Dixon, B. Mortimer, Permutation Groups, Springer, New York, Berlin, Heidelberg, Graduate Texts in Mathematics, vol. 163, 1996.
[5] E. Dobson, Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$, Discrete Math. 147 (1995) 87–94.
[6] E. Dobson, On solvable groups and circulant graphs, European J. Combin. 21 (2000) 881–885.
[7] B. Fein, W.M. Kantor, M. Schacher, Relative Brauer groups II, J. Reine Angew. Math. 328 (1981) 39–57.
[8] G. Gamble, C.E. Praeger, Vertex-primitive groups and graphs of order twice the product of two distinct odd primes, J. Group Theory 3 (2000) 247–269.
[9] M. Giudici, Quasiprimitive groups with no fixed point free elements of prime order, J. London Math. Soc. 67 (2003) 73–84.
[10] D. Gorenstein, Finite Groups, Chelsea Publishing Company, New York, 1968.
[11] M. Hall, The Theory of Groups, Chelsea Publishing Company, New York, 1976.

[12] A. Hassani, M. Iranmanesh, C.E. Praeger, On vertex-imprimitive graphs of order a product of three distinct odd primes, J. Combin. Math. Combin. Comput. 28 (1998) 187–213.
[13] M. Iranmanesh, C.E. Praeger, On non-Cayley vertex-transitive graphs of order a product of three primes, J. Combin. Theory Ser. B 81 (2001) 1–19.
[14] C.H. Li, A. Seress, The primitive permutation groups of squarefree degree, Bull. London Math. Soc. 35 (2003) 635–644.
[15] D. Marušič, On vertex symmetric digraphs, Discrete Math. 36 (1981) 69–81.
[16] D. Marušič, Cayley properties of vertex symmetric graphs, Ars Combin. 16-B (1983) 297–302.
[17] D. Marušič, R. Scapellato, Characterizing vertex-transitive *pq*-graphs with an imprimitive automorphism subgroup, J. Graph Theory 16 (1992) 375–387.
[18] D. Marušič, R. Scapellato, Imprimitive representations of $SL(2, 2^k)$, J. Combin. Theory Ser. B 58 (1993) 46–57.
[19] D. Marušič, R. Scapellato, Permutation groups, vertex-transitive digraphs and semiregular automorphisms, European J. Combin. 19 (1998) 707–712.
[20] D. Marušič, R. Scapellato, B. Zgrablić, On quasiprimitive *pqr*-graphs, Algebra Colloq. 2 (1995) 295–314.
[21] B. McKay, C.E. Praeger, Vertex-transitive graphs which are not Cayley graphs I, J. Austral. Math. Soc. Ser. A 56 (1994) 53–63.
[22] B. McKay, C.E. Praeger, Vertex-transitive graphs that are not Cayley graphs II, J. Graph Theory 22 (1996) 321–334.
[23] C.E. Praeger, M.Y. Xu, Vertex-primitive graphs of order a product of two distinct primes, J. Combin. Theory Ser. B 59 (1993) 245–266.
[24] A. Seress, On vertex-transitive, non-Cayley graphs of order *pqr*, Discrete Math. 182 (1998) 279–292.
[25] H. Wielandt, Permutation groups through invariant relations and invariant functions, Lecture Notes, Ohio State University, Columbus, 1969.